Exhibit I

Exhibit 5

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Alexandria Division

UNITED STATES OF AMERICA, Plaintiff, v. ZACKARY ELLIS SANDERS, Defendant.	Case No. 1:20-cr-00143 Honorable T.S. Ellis, III

Second Declaration of Anthony J. Ferrante

I, Anthony J. Ferrante, declare under the penalty of perjury that:

1. I am a Senior Managing Director and Global Head of Cybersecurity at FTI Consulting. I have more than 25 years of top-level cybersecurity experience. My curriculum vitae is attached as Exhibit A.

2. Before joining FTI Consulting, I served as Director for Cyber Incident Response at the U.S. National Security Council at the White House, where I coordinated U.S. responses to unfolding domestic and international cybersecurity crises and issues. As a director, I led the development and implementation of Presidential Policy Directive 41 – United States Cyber Incident Coordination, the federal government's national policy guiding cyber incident response efforts.

3. Before being detailed by the Federal Bureau of Investigation ("FBI") to the National Security Council, I served as Chief of Staff for the FBI's Cyber Division. I originally entered on duty to the FBI as a Special Agent in 2005, when I was assigned to the FBI's New York Field Office. In 2006, I was selected as a member of the FBI's Cyber Action team, a fly-team of experts who deploy globally to respond to the most critical cyber incidents on behalf of the U.S. Government. My work at the FBI included liaising with international partners, including regarding intelligence-sharing and on joint investigations.

4. I received a Bachelor of Science in Computer Science from Fordham University, a Master of Science in Computer Science from Fordham University, a Certificate in *Cybersecurity: The Intersection of Policy and Technology* from Harvard University, and a Certificate in *Cybersecurity Strategy* from Georgetown University.

5. I have been retained as an expert by Mr. Sanders's defense team because of my expertise in data privacy, cybersecurity, forensic technology, and global law enforcement investigations, including the specific policies and practices of the FBI in investigating cyber incidents and online conduct.

6. I have reviewed relevant discovery in this case, including but not limited to the purported three "tip" documents the [redacted] provided to the FBI, the FD-1057 that Special Agent Christopher Ford ("Special Agent Ford") completed on January 17, 2020, to open the FBI Washington Field Office's investigation into IP address 98.169.118[.]39, and Special Agent Ford's Affidavit in Support of the Search Warrant.

7. Based on my 12 years of investigative experience as an FBI Special Agent, I am very familiar with the processes and documents required to open an investigation in accordance with requirements detailed in the Domestic Investigation Operations Guide ("DIOG"). Based on this experience, I know for a fact all information relating to the case must be appropriately documented within the SENTINEL "case file." As a matter of FBI policy, all material supporting a case must be properly documented to the case file. In some situations, some material may require a corresponding cover communication (e.g., FD-302, or FD-1057). All information contained within a SENTINEL case file is serialized for appropriate tracking and referencing in support of the investigation.

8. Based on my review of the discovery in this case and my understanding of FBI policy and practice, there are likely outstanding materials that exist in the FBI's possession relevant to the identification of IP address 98.169.118[.]39, the activity of a user of IP address 98.169.118[.]39, the documentation surrounding the "tip" from the [redacted], and material related to the investigation into the site, [redacted]

9. Based on my review of the purported "tip" document provided by the [redacted] with the report title "CSAE Imagery on Tor Hidden Service Site [redacted]" it appears as though documents such as these were sent to multiple international partner agencies with knowledge of the broader [redacted] operation. I make this statement based upon the box within the report containing "Disseminated to: International partners in receipt of [redacted]" Based on my experience as an FBI Special Agent, the three purported "tip" documents that the [redacted] allegedly provided to the FBI would have followed a defined process. Specifically, the [redacted] would have sent the documents to a point of contact at FBI Headquarters, who would then have then routed to the appropriate FBI Field Office squad for further investigation.

10. The FBI opened its investigation into IP address 98.169.118[.]39 on January 17, 2020, when Special Agent Ford filed an electronic communication known as an "EC" or "FD-1057." *See* FD-1057, attached as Ex. B, at 1. The opening EC is required to open an investigation and constitutes the first document (*i.e.,* the first "Serial") in that case file. The investigation into IP address 98.169.118[.]39 was assigned Case ID#s [redacted] and [redacted]. The letters "WF" in these case numbers reveal that this is an investigation run by the FBI's Washington Field Office. Special Agent Ford's

opening EC is "Serial 1" in [redacted] and [redacted], because it is the first document in those case files. The case file number and phrase "Serial 1" appears atop each page of the opening EC. Exhibit B at 1-4. The second document added to those case files would be Serial 2 (and would have case file number and phrase "Serial 2" written across the top of each page), the third would be Serial 3 (and would have case file number and phrase "Serial 3" written across the top of each page), and so on.

11. The Washington Field Office case regarding IP address 98.169.118[.]39 was opened in reference to a pre-existing case file managed by FBI Headquarters, which had already been assigned Case ID# [redacted] and was opened on or prior to September 10, 2019. Ex. B at 2. I can say this with complete certainty because Special Agent Ford's opening EC for IP address 98.169.118[.]39 lists "[redacted] Serial 44" as a "Reference," Ex. B at 1, and also refers to "[redacted] Serial 257," Ex. B at 2. The letters "HQ" in that case number signify that FBI HQ was responsible for managing the case file. The phrase [redacted] in "[redacted] Serial 44" refers to the specific [redacted] sub-file of that case file managed by Headquarters. Serial 44 refers to the 44th document in the [redacted] subfile. The letters "SBP" in "[redacted]-SBP" typically refer to the "Subpoena" subfile of the case file. Serial 257 refers to the 257th document added to the "Subpoena" subfile of the case file.

12. Based on my experience and review of the opening EC, I believe that the WFO investigation of IP address 98.169.118[.]39 ([redacted] and [redacted]) was opened as a "Spin-Off" investigation stemming from a case managed by FBI HQ ([redacted]). Headquarters would generally not run an investigation into a single individual potentially suspected of possessing or distributing child pornography. In my experience at both an FBI Field Office and FBI HQ, Headquarters is typically responsible for providing programmatic guidance, or leading and coordinating large-scale operations requiring national and/or international coordination, including working with FBI Legal Attaches (LEGATs) and partner law enforcement agencies. This is because Headquarters, as the name suggests, is very different from a field office, including the Washington Field Office. The responsibility of FBI HQ is to provide strategic guidance and centralized coordination between the 56 Field Offices and 60 LEGAT offices.

13. As part of [redacted], Headquarters issued administrative subpoenas in the larger investigation, including on September 10, 2019. Ex. B at 2. In my experience, Headquarters would normally only issue administrative subpoenas to add efficiencies and aide the field following the receipt of information from national and international partner agencies.

14. The administrative subpoena issued on September 10, 2019, was issued by Headquarters in reference to the larger investigation [redacted], rather than by the Washington Field Office in reference to the investigation of IP address 98.169.118[.]39 ([redacted] and [redacted]).

15. Because the opening EC for the investigation of IP address 98.169.118[.]39 references "[redacted] Serial 44" and "[redacted] SBP Serial 257," at the time the investigation into IP address 98.169.118[.]39 was opened on January 17, 2020, there were already, at minimum, Serials 1 through 44 in the "[redacted]" subfile, for a total of at least 44 documents. In addition, there were already, at minimum, Serials 1 through 257 in the "SBP" (Subpoena) subfile, for a total of at least 257 documents.

16. It appears that versions of the of the three purported [redacted] "tip" documents which the United States Government provided to the defense have not been serialized. Furthermore, it is not apparent that any of those three "tip" documents are referenced in the opening EC of the investigation of IP address 98.169.118[.]39 ([redacted] and [redacted]). Thus, these "tip" documents either (1) are not part of any case file, whether the case file managed by Headquarters or the investigation into IP address 98.169.118[.]39 run by the Washington Field Office; or (2) were uploaded into SENTINEL only as attachments to serialized documents, such as an FBI FD-302. Notably, Special Agent Ford's opening EC refers in the "Reference" line to a [redacted] Serial 44," Ex. B at 1, raising the possibility that one or more of the purported tip documents may be appended to that serialized document.

17. Special Agent Ford's FD-1057 provides: "In August 2019, the FBI received information from a foreign law enforcement agency (FLA) known to the FBI with a history of providing reliable, accurate information in the past that FLA identified a user who accessed [redacted] using IP address 98.169.118[.]39, on May 23, 2019, at 02:06:48 UTC. The FLA obtained the information using methods that were legal in that country. Furthermore, the FLA did not access any devices in the United States in order to provide this information." Ex. B at 2. This paragraph does not contain any reference to another Serial. Based on my knowledge of FBI policy and practice, I know that if this paragraph was based on any of the three "tip" documents, the Serials for those documents should have been referenced within that paragraph.

18. At the time Special Agent Ford opened the investigation into IP address 98.169.118[.]39, he stated, "FBI database queries[1] for IP address 98.169.118[.]39 revealed nothing pertinent." Ex. B at 3. This is significant because Special Agent Ford identified multiple databases in which he queried and stated there was nothing "pertinent," such as an FLA lead, or any documentation surrounding the alleged suspicious or illegal activity.

19. Based on all of the above, and my knowledge and expertise with respect to FBI policy and practice, the following additional documents certainly exist in the FBI's possession that are related to the overarching Headquarters initative, and specific information related to the investigation of IP address 98.169.118[.]39, how it was identified, what evidence there was as to what activity a user of that IP address had engaged in on May 23, 2019, and what Special Agent Ford understood when he opened the investigation into that IP address:

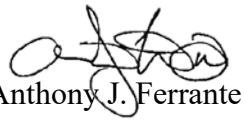
[1] Contained within the Opening EC the FBI identifies the following databases were searched: Accurint, CLEAR, National Crime Information Center (NCIC), National Data Exchange (N-DEx), National Sex Offender Public Website (NSOPW), the public Internet.

a. [redacted] Serial 1 (the opening EC for the larger investigation).
b. [redacted] – [redacted] Serial 44 (the 44th document in the "[redacted]" subfile, which is referenced in Special Agent Ford's 1057).
c. [redacted] – [redacted] Serials containing IP address "98.169.118[.]39."
d. [redacted] – [redacted] Serials containing information about Risa Sanders, the Sanders family home, Zackary Sanders, or Jay Sanders.
e. [redacted] – SBP Serials containing IP address "98.169.118[.]39."
f. [redacted] – SBP Serials containing information about Risa Sanders, the Sanders family home, Zackary Sanders, or Jay Sanders.
g. [redacted] – SBP Serial 257 (the 257th document in the "SBP" subfile, which is referenced in Special Agent Ford's 1057).
h. [redacted] Serials in the main case file and subfiles mentioning "98.169.118[.]39" and/or information about Risa Sanders, the Sanders family home, Zackary Sanders, or Jay Sanders.
i. [redacted] or [redacted] Serials that have not yet been provided.

20. I would expect the following documents to be contained within SENTINTEL as additional evidence to support the case against the defendant, if they exist:
    a. Any documentation, such as an MLAT and/or MOU, used as the basis for the receipt and sharing of information between the U.S. and [redacted] related to these types of matters.
    b. Additional materials provided by the [redacted] to the FBI that identify or discuss IP address 98.169.118[.]39, including the presence or absence of log data and device identifying information.
    c. The serials and case file numbers that the three "tip" documents were assigned.
    d. Additional reports and serials within FBI databases and/or partner agencies that contain IP address "98.169.118[.]39."
    e. Additional reports and serials identifying device identification information associated with IP address "98.169.118[.]39," including MAC address, user-agents, browser type, and device types.

21. I would expect the FBI to have evidence that a specific IP address viewed, downloaded, or uploaded specific illegal files, and understand how that IP address was identified before the FBI opened an investigation into a specific IP address or sought a search warrant. From the discovery provided to date, it does not appear the FBI has conclusively tied a user from the IP address 98.169.118[.]39 to the actions outlined in the opening EC. The absence of technical evidence (e.g., network traffic logs, named images or videos, et cetera.) to corroborate the tip suggests, however, that there was no such information, which is concerning. Indeed, as described above, there were no results, in databases that the FBI had access to, that IP address 98.169.118[.]39 had ever engaged in suspicious or illegal activity.

DONE this 30th day of July 2021.



Anthony J. Ferrante

Exhibit A

Anthony J. Ferrante

Global Head of Cybersecurity
Senior Managing Director

555 12th Street NW, Suite 700 - Washington, DC 20004
+1 202 312 9165
ajf@fticonsulting.com

Education

M.S. and B.S., Computer Science, Fordham University

Cybersecurity Policy, Harvard University, John F. Kennedy School of Government

Cybersecurity Strategy, Georgetown University

Expertise

Crisis Management
Cyber Incident Coordination
Cybersecurity Preparedness
Cybersecurity Policy and Compliance
Data Privacy
Host-based Digital Forensics
Incident Response
Investigations
Network Forensics
Malware Analysis
Network Security
Source Code Auditing and Review
Threat-hunting
Vulnerability Assessments

Coding Languages

JavaScript, C++, HTML, PEARL, Python, Visual Basic

Security Clearance

Active TOP SECRET/SCI

Mr. Ferrante is an expert in data privacy, compliance, and cybersecurity readiness, prevention, incident response, remediation, recovery, and complex investigation services.

Mr. Ferrante has more than 25 years of top-level cybersecurity experience, providing incident response and readiness planning to more than 1,000 private sector and government organizations, including over 175 Fortune 500 companies and 70 Fortune 100 companies. Further, Mr. Ferrante is versed in cybersecurity regulation and legislation, including DFARS, HIPAA, ITAR, GDPR, CCPA, NYDFS, and PCI DSS.

Mr. Ferrante maintains first-hand operational knowledge of more than 60 criminal and national security cyber threat sets, and extensive practical expertise researching, designing, developing, and hacking technical applications and hardware systems, allowing for unparalleled client advisory and support in complex investigations and litigation.

Prior to joining FTI Consulting, Mr. Ferrante served as Director for Cyber Incident Response at the U.S. National Security Council at the White House where he coordinated U.S. response to unfolding domestic and international cybersecurity crises and issues. Building on his extensive cybersecurity and incident response experience, he led the development and implementation of Presidential Policy Directive 41 – United States Cyber Incident Coordination, the federal government's national policy guiding cyber incident response efforts.

Before joining the National Security Council, Mr. Ferrante was Chief of Staff of the FBI's Cyber Division. He joined the FBI as a special agent in 2005, assigned to the FBI's New York Field Office. In 2006, Mr. Ferrante was selected as a member of the FBI's Cyber Action Team, a fly-team of experts who deploy globally to respond to the most critical cyber incidents on behalf of the U.S. Government.

Mr. Ferrante was an Adjunct Professor of Computer Science at Fordham University's Graduate School of Arts and Sciences, where he served as the founder and co-director of the Master's of Science in Cybersecurity Program in the Graduate School of Arts and Sciences. During his time at Fordham University, he served as the co-director of the undergraduate and graduate cybersecurity research program.

Mr. Ferrante received the 2019 Global Leaders in Consulting award for his Excellence in Execution from *Consulting* Magazine. Additionally, in 2019, Mr. Ferrante and FTI Consulting were invited to partner with the World Economic Forum's Centre for Cybersecurity to strengthen global cooperation for digital trust and security, secure future digital networks and technology, and build skills and capabilities for the digital future. In August 2019, Mr. Ferrante summited Mount Kilimanjaro, the highest mountain in Africa and the highest single free-standing mountain in the world.

Expert Retention

- United States International Trade Commission, Investigation No. 337-TA-1159. **In The Matter Of CERTAIN LITHIUM ION BATTERIES, BATTERY CELLS, BATTERY MODULES, BATTERY PACKS, COMPONENTS THEREOF, AND PROCESSES THEREFOR.** Expert witness for LG Chem Ltd. regarding cybersecurity measures.
- United States District Court for the Southern District of Florida Miami Division (Case No. 1:17-CV-60426-UU). Aleksej Gubarev, XBT Holdings S.A., and Webzilla, Inc., Plaintiffs, v. **Buzzfeed, Inc. and Ben Smith, Defendants.** Expert report issued May 2018. Deposition taken July 2018.
- United States District Court for the Northern District of California (Case No. 16-MD02752-LHK) **Yahoo! Inc. Customer Data Security Breach Litigation.** Expert report issued September 2018.

Awards

- Data 2021 - Data Experts, *Who's Who Legal* (2020)
- Global Leaders in Consulting, Excellence in Execution, *Consulting* Magazine (2019)
- Tech 25 innovators & Disruptors, *Washington Life* (2019)

Notable Professional Activities

- Founder, Federal Bureau of Investigation Chief Information Security Officer (CISO) Academy, September 2015
- Co-Founder, Master's Degree in Cyber Security at Fordham University, September 2012
- Founder, International Conference on Cyber Security, Fordham University, January 2007

Featured Media Appearances

- CNN, *Analyst explains why hospitals are vulnerable to hackers*, October 2020
- CNN, *Feds: Russia & Iran Have Interfered with Presidential Election*, October 2020
- CNN, *Here's How Iran Could Bring This Fight into American Homes*, January 2020
- CNN, *DHS May Update Terror Threat Advisory After U.S. Killing of Top Iranian General*, January 2020
- CNN, *Police: Six Officers Shot in Philadelphia*, August 2019
- CNN, *FBI: Dayton Shooter Was Exploring Violent Ideologies*, August 2019
- CNN, *Death Toll Rises to 31 in Mass Shootings*, August 2019
- CNN, *Senate Report: Russia Targeted All 50 States in 2016 Election*, July 2019
- CNN, *Senate Intel Report Details Russia's Wide-Ranging Election Interference in 2016*, July 2019
- CNN, *"Person of Interest" in Student's Disappearance*, June 2019
- CNN, *At Least 12 Dead in Mass Shooting in Virginia Beach*, May 2019
- CNN, *"Close Collaborator" of Assange Under Arrest*, April 2019
- CNN, *Wikileaks Founder Julian Assange Facing Extradition to U.S. on Conspiracy Charge After Dramatic Arrest in London*, April 2019
- CNN, *Experts Detail Alleged Intruder's Sophisticated Tools*, April 2019
- CNN, *Manhunt for Serial Bomber Behind Mass Assassination Attempt*, October 2018
- 60 Minutes, *When Russian hackers targeted the U.S. election infrastructure*, April 2018

- CNN, *Special Report: The Trump-Russia Investigation*, January 2018
- Expansión Newspaper (Spain), *Cybercriminals act every day of the year*, November 2017
- Bloomberg Tech TV, *Equifax Data Breach*, September 2017
- National Public Radio, *Russian Cyberattack Targeted Elections Vendor Tied To Voting Day Disruptions*, August 2017
- Time Magazine, *Inside the Secret Plan to Stop Vladimir Putin's U.S. Election Plot*, July 2017
- Bloomberg Tech TV, *Hackers Find Flaws in Voting Machines*, July 2017

Recent Publications

- The Hill, *The US presidential election is under attack*, October 2020
- The Hill, *States Must Take Action to Protect Against Unemployment Fraud*, June 2020
- Law360, *9 Post-Coronavirus Cybersecurity Predictions for Cos.*, June 2020
- The Hill, *COVID-19: Attempts to Influence and Deceive*, April 2020
- The Hill, *2020 Cybersecurity Predictions: Evolving Vulnerabilities on the Horizon*, January 2020
- The Hill, *Playing With Fire: Global Offensive Cyber Operations*, October 2019
- High Performance Counsel, *Business Email Compromise: How To Avoid Becoming A Victim*, April 2019
- Corporate Compliance Insights, *10 Corporate Cybersecurity Predictions What You Need to Know for 2019 - and Beyond*, February 2019
- Cyber Security: A Peer-Reviewed Journal, *The Impact of GDPR on WHOIS: Implications for Businesses Facing Cybercrime*, July 2018
- Corporate Board Member, *The Insiders: Cybersecurity*, April 2018
- CSO Online, *3 Top Cyber Experts Speaking Out*, January 2018
- Yahoo! News, *Cyberwar is our era's Cuban missile crisis. We need to de-escalate, now*, November 2017
- Power Magazine, *Why CrashOverride Is a Red Flag for U.S. Power Companies*, November 2017
- New York Law Journal, *Vulnerability Management: A Holistic View*, October 2017
- Insurance Journal, *What Insurance Companies Need to Know About Part 500 Cybersecurity Compliance*, October 2017
- Risk Management Magazine, *Enhancing Security with Big Data Analytics*, October 2017
- Information Systems Security Association Journal, *Battening Down for the Rising Tide of IoT Risks*, August 2017

Notable Speaking Engagements

- Securities Enforcement Forum 2020, *Cybersecurity and Cryptocurrency Regulation, Enforcement and Litigation*, Webinar, October 2020
- ABA Cybersecurity, Privacy and Data Protection Committee, *Cyber-Related Litigation and Best Practices for Incident Preparedness and Response*, Webinar, August 2020
- International Association of Privacy Professionals, *The New Normal: Navigating "Work From Home" Privacy and Cybersecurity Risks,* Webinar, May 2020
- AICPA Forensic & Valuation Services Conference, *A Look into the Future of Blockchain Litigation*, Las Vegas, NV, October 2019
- Institutional Investor Legal Forum Fall Roundtable, *Cybersecurity: Confronting an Existential Threat*, Washington, DC, November 2019

- Privacy + Security Forum, *Best Practices for Preparing a Ransomware-Related Cyber Incident Response Plan*, Washington, DC, October 2019
- Kirkland & Ellis, *Cybersecurity Trends Impacting Healthcare Businesses*, New York, NY October 2019
- DEF CON 27, *Coffee Talk with Anthony Ferrante*, Las Vegas, NV, August 2019
- ICCS, *The Tipping Point: Cyber Risks to Election Systems*, New York, NY, July 2019
- Security & Risk Leadership Academy, *Anything You Say Can and Will Be Used Against You*, Skytop, PA, June 2019
- Securities Enforcement Forum West, *Cybersecurity Disclosure and Enforcement: Will the SEC Drop the Hammer in 2019*, East Palo Alto, CA, May 2019
- Spark Leadership Forum, *Anything You Say or Do May Be Used Against You*, Napa, CA April 2019
- Greenberg Traurig, *Cybersecurity Incident Response and Crisis Management Seminar*, New York, NY, March 2019
- RSA Conference, *AI: Hacking without Humans How Can Human Brains Be Hacked?*, San Francisco, CA, March 2019
- RSA Conference, *Investigating IoT Crime: The Value of IoT Crime Classification*, San Francisco, CA, March 2019
- The Americas Lodging Investment Summit Law Conference, *Battling Cybersecurity Challenges & Elevating Cybersecurity Posture*, Los Angeles, CA, January 2019
- World Economic Forum's Centre for Cybersecurity, *Why We Need Global Cyber Response Principles*, Geneva, Switzerland, November 2018
- U.S.-China Economic and Security Review Commission, *Hearing on China, the United States, and Next Generation Connectivity*, Washington, DC, March 2018
- ILS Forum on International Law, *Digital Currencies in a Connected World*, Miami, FL, February 2018
- Bloomberg, *In-House Counsel's Growing Role in Cybersecurity Risk Management*, Washington, DC, January 2018
- The Conference Board, *Cybersecurity: Crucial Collaborations*, New York, NY, January 2018
- IESE Global Alumni Reunion, *New Rules in Cybersecurity*, Madrid, Spain, November 2017
- Perez-Llorca, *Cybersecurity Panel*, Madrid, Spain, November 2017
- IAWatch, *Incident Response: Planning for and Reacting to Potential Events*, Washington, DC, October 2017
- Federal Bar Association, *Litigating Cybersecurity and Defending Privacy Class Actions*, Atlanta, GA, September 2017
- Compliance Governance Oversight Council, *Cybersecurity Landscape*, Minneapolis, MN, June 2017
- Hogan Lovells, *Ready, Set, Respond*, Washington, DC, September 2016
- PKF O'Connor Davies, *Financial Issues and Trends Affecting Your Club*, New York, NY, May 2013
- Coalition Against Domain Name Abuse, *The Evolution of Cybercrime*, Washington, DC, October 2010
- National Committee on American Foreign Policy, *Cyber War: Perception, Reality, and Strategy*, New York, NY, October 2010

Exhibit B

FD-1057 (Rev. 5-8-10)

UNCLASSIFIED

FEDERAL BUREAU OF INVESTIGATION

Electronic Communication

Title: (U) Opening EC **Date:** 01/17/2020

CC: D6-VCACU (UC)
Christina M Bedford

From: WASHINGTON FIELD
WF-CR18
Contact: FORD CHRISTOPHER A, [redacted]

Approved By: SSA Barbara B. Smith

Drafted By: FORD CHRISTOPHER A

Case ID #: [redacted] (U) 98.169.118.39 - TOR [redacted];
VICTIM - UNKNOWN, MCLEAN, VA;
DISTRIBUTION OF CHILD PORNOGRAPHY;

Synopsis: (U) To document the case opening

Reference: [redacted] Serial 44

Details:

[redacted] was an online bulletin board dedicated to the advertisement and distribution of child pornography that operated from approximately 2016 to June 2019. On the site's announcements page was the following text: "this website was created to host videos, photos and discussions of 18 (twinks) and younger of Hurtcore materials (videos & pictures) as well as discussion of such."

On June 23, 2016, a site administrator posted a topic entitled "Board Rules" in the "Important Information" forum which contained the following explanation of the site: "[redacted]

UNCLASSIFIED

Title: (U) Opening EC

Re: [redacted], 01/17/2020

[redacted]

[redacted]

In August 2019, the FBI received information from a foreign law enforcement agency (FLA) known to the FBI with a history of providing reliable, accurate information in the past that FLA identified a user who accessed [redacted] using IP address 98.169.118.39, on May 23, 2019, at 02:06:48 UTC. The FLA obtained the information using methods that were legal in that country. Furthermore, the FLA did not access any devices in the United States in order to provide this information.

On September 10, 2019, an administrative subpoena was issued to Cox Communications for information related to IP address 98.169.118.39, on May 23, 2019, at 02:06:48 UTC. Cox Communications provided the following subscriber information (refer to [redacted] Serial 257):

Name: Risa Sanders
Address: 7850 Westmont Lane, Mclean, VA 22102-1452
Telephone: [redacted]
Account Status: Active

Title: (U) Opening EC
Re: [redacted], 01/17/2020

An Accurint search for Risa Sanders at 7850 Westmont Lane, McLean, VA 22102 yielded the following results: Risa Edwards Sanders (DOB: [redacted]/1957; SSN: [redacted]). Accurint revealed the following names for Sanders: Risa J. Edwards, Risa J. Sanders, Re E. Sanders, and Rita E. Sanders. Accurint reported the phone number(s) associated to this address as [redacted]. Accurint reported the following current residents at this address: Jay H. Sanders (DOB: [redacted]/1988; SSN: [redacted]) and Zackary E. Sanders. Risa Sanders is licensed clinical psychologist.

A Clear search with the same search parameters confirmed the address. Clear also provides the following additional name for Sanders Risa H. Sanders; additional DOB for Sanders as [redacted]/1957; and additional information for Zackary E. Sanders: (DOB: [redacted]1995; SSN: [redacted]). Clear reports that Sanders has two emails: [redacted]@early.com and [redacted]@gmail.com.

An NCIC search for a criminal history record for Risa Sanders was negative.

NCIC Mobility searches for a driver's license(s) (DLs) for Risa Sanders were positive for a current license in VA which expires [redacted]2020. Sanders DOB on her DL is [redacted]/1957.

NDEX name, SSN, and DOB searches for Risa Sanders were positive for a speeding violation.

NSOPW searches for Risa Sanders yielded negative results.

FBI database queries for Risa Sanders with SSN and DOB were negative.

FBI database queries for IP address 98.169.118.39 revealed nothing pertinent.

UNCLASSIFIED

Title: (U) Opening EC
Re: [redacted] 01/17/2020

Open source searches for Risa Sanders in McLean VA yielded positive results. According to her website, Sanders is a clinical psychologist who works with adults and children over age six. Her email address [redacted]@early.com) is possibly associated to Amazon, Apple, Google, SoundCloud, Twitter, Venmo, WordPress, and LinkedIn accounts. Sanders phone number [redacted] is possibly associated to a Skype and WhatsApp accounts. No additional derogatory information was revealed.

Based on the provided information, the user of the IP address 98.169.118.39 is in violation of 18 U.S.C 2252(a)(2) Sexual Exploitation of Children, specifically distribution of child pornography.

♦♦